UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,873	05/24/2001	Amiran Ofir	OFIR=1	9480

1444 7590 10/06/2004

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,873	OFIR, AMIRAN	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-4, 6, 7, 15, 15, 19-23 rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak et al., US Patent No 6289450 (hereafter referred to as '450) in view of Kurn et al., US Pre-grant Pub No 20020071567 (hereafter referred to as '567).

3. As to claim(s) 1, 11, 15, 19-23:

'450 teaches a database storage and encrypted communications system comprising:

- Receiving from a user a login request / User is logged into the remote server (Col 8, Line 21, '450)
- Login request includes identifier of user and supplementary data that may be used to authenticate the user / viewing users computer provides login and authentication information to the server (Col 8, Line 26, '450)
- Verifying if the user is a registered user / server determines if viewing user is authorized to access the document segment (Col 8, Line 31, '450

- Receiving a request by the registered user for performing a data operation / application interface requests access to the document or information (Col 8, Line 27, '450)
- Operation together with a session ID known allocated to the user during login and known to the login server / Communicating the session ID of said user to the login server for identification / An SSL tunnel and session key are negotiated (Col 8, Line 23, '450)
- Decrypting encrypted password received form login server to derive password / user provides login and authentication information in encrypted SSL tunnel (Col 8, Lines 23-26, '450), the database functions may be a distributed or shared database residing on multiple remote servers (Col 8, Line 63, '450)

4. '450 does not teach for the server to store and use the encrypted private key of the registered user having said unique identifier using password. '567 teaches a remote database system storing a users private key encrypted by password based encryption (Page 5, Paragraph 0087, '567). It would have been obvious to a person of ordinary skill in the art at the time of invention to store and use the users private key on the database server as in '567 in the invention of '450. One of ordinary skill in the art would have been motivated to store and use the users private key on the database server as in '567 in the invention of '450 because storing the private key encrypted on the trusted database server defers the need to send the private key to the server for every session while maintaining a high level of security.

5. As to claim(s) 2, 6:

Supplementary data serves as said password / Using the supplementary data to generate said password / viewing computer provides login and authentication information (Col 8, Line 26, '450) database is password protected (Col 9, Line 1, '450)

6. As to claim(s) 3, 7:

Encrypting the password so as to generate an encrypted password / user provides login and authentication information in encrypted SSL tunnel (Col 8, Lines 23-26, '450)
Sending the encrypted password to a login server coupled to data access server for storage / viewing computer provides login and authentication information to server (Col 8, Line 26, '450)
Data access server may access the password from the login server without storing it locally / the database may be a distributed or shard database residing on multiple remote servers (Col 8, Line 63, '450)

7. As to claim(s) 4:

Encrypted password sent to the login server is adapted for temporary storage for a current session only / login and authentication information (password) are encrypted under a session key and sent to server (Col 8, Line 24, '450) for current session.

8. Claim 5, 8-10, 12, 16-18 rejected under 35 U.S.C. 103(a) as being unpatentable over '450 in view of '567 in further view of "Group Sharing and Random access in Cryptographic Storage File Systems" (hereafter referred to as CSFS).

As to claim(s) 5, 12:

9. '450 as modified above teaches a distributed function multiple server database storage system and encrypted communications and storing and using private keys encrypted with passwords after a login. '450 as modified above does not teach to inform the login server upon termination of the current session to delete temporarily stored encrypted password. CSFS teaches an encrypted file system using temporary passwords to acquire encryption keys where the user enters the password each time the user logs in (Page 20, Line 12, CSFS). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the once-per-login temporary password system of CSFS with the invention of '450 as modified above. One of ordinary skill in the art would have been motivated to use the once-per-login temporary password system of CSFS with the invention of '450 as modified above because it is easier on the user not to need to enter a password for each encryption operation.

10. '450 as modified above does not teach for the database to delete the temporarily stored encrypted password upon termination of the current session. The examiner takes official notice as to deleting the temporarily stored encrypted password at upon termination of the current session. The temporarily stored password of CSFS is only needed during the current session, and it is a good secure disk management policy to delete temporary security data when it is no longer needed. It would have been obvious

to a person of ordinary skill in the art at the time of invention to delete the session password at the end of the user session. One of ordinary skill in the art would have been motivated to delete the session password at the end of the user session because deleting temporary security data as soon as it is no longer needed provides a greater level of security in that the password is less easily compromised once deleted.

11. As to claim(s) 8, 14:

Sending the unique identity of the user to the login server / User name provided to the remote server (Col 3, Line 63, '450)

Receiving the password from the login server / the database functions may be a distributed or shared database residing on multiple remote servers (Col 8, Line 63, '450)

12. As to claim(s) 9:

'450 as modified above teaches a distributed function multiple server database storage system and encrypted communications and storing and using private keys encrypted with passwords after a login. '450 as modified above does not teach for communication between servers to use encryption. '450 further teaches the use of encrypted SSL communication using public key techniques to transfer data from the server to the user. It would have been obvious to a person of ordinary skill in the art at the time of invention to use SSL for remote server-server communication as used in '450 for server-user communication. One of ordinary skill in the art would have been motivated to use SSL for remote server-server communication as used in '450 for server-user communication

because unencrypted remote communication across insecure networks can result in breaches of security.

13. As to claim(s) 10:

Generating a fingerprint of the password and comparing with a fingerprint stored in the user space associates with the registered user / SSL communication uses data hashing algorithms such as MD5 (Page 3, Line 6, Introduction to SSL)

14. As to claim(s) 16, 17, 18:

Decrypting the users encrypted password using login servers private key / An SSL tunnel is negotiated (Col 8, Line 23, '450) between user and server

Encrypting using a temporary/session/periodically changed key stored in RAM and saving the password / password is re-encrypted for SSL transmission to remote distributed server under temporary SSL session key

15. Claim 13 rejected under 35 U.S.C. 103(a) as being unpatentable over '450 in view of '567 in further view of CSFS in further view of "Manpage of TCSH".

As to claim(s) 13:

'450 as modified above teaches a distributed function multiple server database storage system and encrypted communications and storing and using private keys encrypted with passwords after a login and deleting temporarily stored encrypted passwords after logout. '450 does not teach for a user to be logged out after a timeout period. Manpage

of TCSH teaches a Unix shell that logs off a user after a predetermined time (Page 2, Item 9, Manpage of TCSH). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the automatic logoff after a period of idle time as in "Manpage of TCSH" in the invention of '450 as modified above. One of ordinary skill in the art would have been motivated to use the automatic logoff after a period of idle time as in "Manpage of TCSH" in the invention of '450 as modified above because using an idle timeout helps users logout if they become unable to by normal means such as in the event of a break in connection etc.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (571)272-3832 after 10/04. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100